Available online at www.sciencedirect.com

SCIENCE DIRECT®

Finite Fields and Their Applications 10 (2004) 24–35

FINITE FIELDS AND THEIR APPLICATIONS

http://www.elsevier.com/locate/ffa

On some classes of optimal and near-optimal polynomial codes

Nuh Aydin[a,*] and Dijen K. Ray-Chaudhuri[b]

[a] *Department of Mathematics, Kenyon College, Gambier, OH 43022, USA*

[b] *Department of Mathematics, The Ohio State University, Columbus, OH 43210, USA*

Received 7 July 2002; revised 14 May 2003

Communicated by N.J.A. Sloane

Abstract

We generalize a recent idea for constructing codes over a finite field $\mathbb{F}_q$ by evaluating a certain collection of polynomials over $\mathbb{F}_q$ at elements of an extension field. We show that many codes with the best parameters presently known can be obtained by this construction. In particular, a new linear code, a $[40, 23, 10]$-code over $\mathbb{F}_5$ is discovered. Moreover, several families of optimal and near-optimal codes can also be obtained by this method. We call a code near-optimal if its minimum distance is within 1 of the known upper bound.

Keywords: Linear codes; Reed–Solomon codes; New bounds

1. Introduction

The purpose of this paper is two-fold: First, we give a generalization of the construction in [4]. The extension is of degree 2 in [4]. We first do here the extensions of degree 3 and then for any prime degree. A different approach for extensions of arbitrary degrees using symmetric polynomials is taken in [3], which appeared after this work was completed. Secondly, we introduce a new method of constructing codes over an arbitrary finite field obtained by evaluating certain polynomials at elements of an extension field (Section 4). In all cases, we obtain codes with parameters which are as good as the parameters of the presently best-known codes (some of which are optimal) on the basis of [1]. In particular, we are able to construct

*Corresponding author. Fax: 740-427-5573.

E-mail addresses: aydinn@kenyon.edu (N. Aydin), dijen@math.ohio-state.edu (D.K. Ray-Chaudhuri).

1071-5797/03/$ - see front matter
doi:10.1016/S1071-5797(03)00042-X

infinite families of linear codes with optimal or near-optimal parameters. We call a code near-optimal if its minimum distance is at most 1 less than the largest possible value. We also find a new linear code over $\mathbb{F}_5$ which improves the known bounds; it is a $[40, 23, 10]_5$-code.

To motivate the construction we recall an alternative description of generalized Reed–Solomon codes. Let $1 \leqslant n \leqslant q$, $1 \leqslant k \leqslant n$ and let

$$P_k = \{f(x) \in \mathbb{F}_q[x]: \deg f(x) < k\}.$$

Choose n distinct elements $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{F}_q$, and n non-zero (not necessarily distinct) elements $v_1, v_2, \ldots, v_n$ in $\mathbb{F}_q$. The generalized Reed–Solomon code is defined by

$$GRS_q(n,k) = \{(v_1 f(\alpha_1), v_2 f(\alpha_2), \ldots, v_n f(\alpha_n)): f(x) \in P_k\}.$$

It is well-known that the code $GRS_q(n,k)$ is a linear code with the parameters $[n, k, n-k+1]_q$ over $\mathbb{F}_q$. Therefore it is an MDS code. However, its length is limited by q. If we try to extend the length by evaluating the polynomials at elements of some extension field of $\mathbb{F}_q$ then the resulting code is no longer over $\mathbb{F}_q$. The idea of the construction described in [4] is to choose a special collection of polynomials over $\mathbb{F}_q$ that return elements in $\mathbb{F}_q$ when they are evaluated at elements of $\mathbb{F}_{q^2}$. We give generalizations to this construction and show examples of codes with good parameters obtained through the new methods.

2. Extensions of degree 3

Let $\mathbb{F}_q$ denote the finite field of order q, for a prime power q. Consider the extension $\mathbb{F}_q \subseteq \mathbb{F}_{q^3}$. Two elements α, β are said to be conjugates over $\mathbb{F}_q$ if they are roots of the same irreducible polynomial over $\mathbb{F}_q$, equivalently if $\beta = \sigma^i(\alpha)$ for some integer i where σ is the Frobenius map $\sigma(x) = x^q$ and generates the Galois group of the extension. This is an equivalence relation on $\mathbb{F}_{q^3}$. The conjugacy classes are of 2 types: For an element $\alpha \in \mathbb{F}_q$, its conjugacy class is the singleton $\{\alpha\}$ and for $\beta \in \mathbb{F}_{q^3} - \mathbb{F}_q$ it is the set $\{\beta, \beta^q, \beta^{q^2}\}$ of size 3. Therefore, we can list the elements of $\mathbb{F}_{q^3}$ as follows:

$$\{\alpha_1, \alpha_1, \ldots, \alpha_q, \beta_1, \beta_1^q, \beta_1^{q^2}, \ldots, \beta_r, \beta_r^q, \beta_r^{q^2}\},$$

where the first q elements constitute $\mathbb{F}_q$ and $r = \frac{q^3-q}{3}$.

An important part of the construction is to define a collection of polynomials over $\mathbb{F}_q$ which return elements of $\mathbb{F}_q$ when evaluated at arbitrary elements of $\mathbb{F}_{q^3}$.

For $0 \leqslant i \leqslant j \leqslant k$, let

$$e_{i,j,k}(x) = x^{q^2 i + qj + k} + x^{q^2 j + qk + i} + x^{q^2 k + qi + j}.$$

When we refer to the polynomial $e_{i,j,k}(x)$, we always assume the condition $0 \leqslant i \leqslant j \leqslant k$.

The important property of $e_{i,j,k}(x)$ is that $e_{i,j,k}(\beta) \in \mathbb{F}_q$ for any $\beta \in \mathbb{F}_{q^3}$. This follows from the fact that $(e_{i,j,k}(\beta))^q = e_{i,j,k}(\beta)$, which can be readily verified.

Now consider the $\mathbb{F}_q$-span $V_{m,3}$ of the set

$$E_{m,3} \coloneqq \{e_{i,j,k}(x)\colon 0 \leqslant i \leqslant j \leqslant k \leqslant m-1\}.$$

Being the $\mathbb{F}_q$-span of $E_{m,3}$, $V_{m,3}$ has the property that $f(\beta) \in \mathbb{F}_q$ for any $f \in V_{m,3}$ and $\beta \in \mathbb{F}_{q^3}$. To find the dimension of $V_{m,3}$, we need to determine the size of $E_{m,3}$. As the degrees of the elements of $E_{m,3}$ are all distinct, we will have $dim(V_{m,3}) = |E_{m,3}|$. This amounts to finding the size of the set $\{0 \leqslant i \leqslant j \leqslant k \leqslant m-1\}$. We will make use of the following well-known combinatorial result.

Proposition 1. *The cardinality of the set* $\{0 \leqslant i_1 \leqslant i_2 \leqslant \cdots \leqslant i_p \leqslant m-1\}$, $p, m \geqslant 1$ *is* $\frac{[m]^p}{p!} = \binom{m+p-1}{p} = \binom{m+p-1}{m-1}$ *where* $[m]^p = m(m+1)\cdots(m+p-1)$ *is called "m rising factorial p".*

Corollary 1. *The dimension of* $V_{m,3}$ *is* $\frac{[m]^3}{3!} = \frac{m(m+1)(m+2)}{6}$.

For $0 \leqslant t \leqslant q$, $1 \leqslant b \leqslant r = \frac{q^3-q}{3}$ and $1 \leqslant m < 1 + \frac{t+3b}{q^2+q+1}$ we define a code $C_3(t,b,m)$ over $\mathbb{F}_q$ as follows:

$$C_3(t,b,m) = \{(f(\alpha_1), \ldots, f(\alpha_t), f(\beta_1), f(\beta_2), \ldots, f(\beta_b)) \,|\, f \in V_{m,3}\}.$$

This is obviously a linear code of length $n = t + b \leqslant q + \frac{q^3-q}{3} = \frac{q^3+2q}{3}$ over $\mathbb{F}_q$.

Proposition 2. *For* $1 \leqslant m < 1 + \frac{t+3b}{q^2+q+1}$, *the dimension of* $C_3(t,b,m)$ *is equal to* $\frac{m(m+1)(m+2)}{6}$.

Proof. The claim follows from the observation that the linear map

$$\phi : V_{m,3} \to \mathbb{F}_q^n$$

$$f \to (f(\alpha_1), \ldots, f(\alpha_t), f(\beta_1), f(\beta_2), \ldots, f(\beta_b)).$$

is one to one. □

Next, we estimate the minimum distance of $C_3(t,b,m)$. The method and the calculations are similar to those used in [4].

Proposition 3. *If the characteristic of $\mathbb{F}_q \neq 3$ then the minimum distance d of $C_3(t,b,m)$ satisfies*

$$d \geqslant n - \frac{1}{3}((q^2+q+1)(m-1) + \max\{3t-2q, 2\cdot\min\{3(m-1), t\}\}).$$

Proof. Let $f(x)$ be an arbitrary polynomial in $V_{m,3}$. Write

$$f(x) = \sum_{s=0}^{3(m-1)} \sum_{\substack{i+j+k=s \\ 0\leqslant i\leqslant j\leqslant k\leqslant m-1}} a_{i,j,k} e_{i,j,k}(x).$$

Case i: $\sum_{\substack{i+j+k=s \\ 0\leqslant i\leqslant j\leqslant k\leqslant m-1}} a_{i,j,k} = 0 \quad \forall 0 \leqslant s \leqslant 3(m-1)$.

$$\begin{aligned} f(x) &= \sum_{s=0}^{3(m-1)} \sum_{\substack{i+j+k=s \\ 0\leqslant i\leqslant j\leqslant k\leqslant m-1}} a_{i,j,k} e_{i,j,k}(x) \\ &= \sum_{s=0}^{3(m-1)} \sum_{\substack{i+j+k=s \\ 0\leqslant i\leqslant j\leqslant k\leqslant m-1}} a_{i,j,k} e_{i,j,k}(x) \\ &\quad - \sum_{s=0}^{3(m-1)} \left(\sum_{\substack{i+j+k=s \\ 0\leqslant i\leqslant j\leqslant k\leqslant m-1}} a_{i,j,k} \right) (x^s + x^{qs} + x^{q^2 s}) \\ &= \sum_{s=0}^{3(m-1)} \sum_{\substack{i+j+k=s \\ 0\leqslant i\leqslant j\leqslant k\leqslant m-1}} a_{i,j,k} \\ &\quad \times (\underbrace{x^{q^2 i+qj+k} + x^{q^2 j+qk+i} + x^{q^2 k+qi+j} - x^s - x^{qs} - x^{q^2 s}}_{p_{i,j,k}(x)}). \end{aligned}$$

One verifies that $p_{i,j,k}(\alpha) = p_{i,j,k}{}'(\alpha) = 0$ for any $\alpha \in \mathbb{F}_q$ ($p_{i,j,k}{}'(x)$ denoting the derivative of $p_{i,j,k}(x)$) so $(x^q - x) | p_{i,j,k}(x)$ and $(x^q - x) | p_{i,j,k}{}'(x)$, hence $(x^q - x)^2 | p_{i,j,k}(x)$. It follows that $(x^q - x)^2 | f(x)$. Let $g(x) := \frac{f(x)}{(x^q - x)^2}$. Then $f(\beta_i) = 0$ if and only if $g(\beta_i) = 0$ since $\beta_i^q - \beta_i \neq 0$. Therefore, $f(x)$ has $\leqslant deg\, g(x)/3$ roots among $\{\beta_1, \beta_2, \ldots, \beta_r\}$ since $g(\beta) = 0$ if and only if $g(\beta^q) = 0$ if and only if $g(\beta^{q^2}) = 0$. So, $f(x)$ has $\leqslant t + deg\, g(x)/3$ roots among $\{\alpha_1, \alpha_2, \ldots, \alpha_t, \beta_1, \beta_2, \ldots, \beta_r\}$, and $wt(\phi(f(x))) \geqslant n - (t + deg\, g(x)/3) \geqslant n - (t + \frac{1}{3}((q^2+q+1)(m-1) - 2q) = n - \frac{1}{3}((q^2+q+1)(m-1) + 3t - 2q)$.

Case ii: Let u be the smallest integer satisfying $0 \leqslant u \leqslant 3(m-1)$,

$$\sum_{\substack{i+j+k=u \\ 0\leqslant i\leqslant j\leqslant k\leqslant m-1}} a_{i,j,k} \neq 0$$

and

$$\sum_{\substack{i+j+k=s \\ 0\leqslant i\leqslant j\leqslant k\leqslant m-1}} a_{i,j,k}=0 \quad \text{for } u<s\leqslant 3(m-1).$$

For $\alpha\in\mathbb{F}_q$, $f(\alpha)=0$ if and only if

$$\sum_{s=0}^{3(m-1)} \sum_{\substack{i+j+k=s \\ 0\leqslant i\leqslant j\leqslant k\leqslant m-1}} 3a_{i,j,k}\alpha^s=0$$

if and only if

$$\sum_{s=0}^{u} \sum_{\substack{i+j+k=s \\ 0\leqslant i\leqslant j\leqslant k\leqslant m-1}} 3a_{i,j,k}\alpha^s=0.$$

So $\alpha\in\mathbb{F}_q$ is a root of $f(x)$ if and only if it is a root of

$$\sum_{s=0}^{u}\left(\sum_{\substack{i+j+k=s \\ 0\leqslant i\leqslant j\leqslant k\leqslant m-1}} a_{i,j,k}\right)x^s=0.$$

Hence, $f(x)$ has at most u roots in $\mathbb{F}_q$, and since $u\leqslant 3(m-1)$, it has at most $\min\{3(m-1),t\}$ roots in $\{\alpha_1,\alpha_2,\ldots,\alpha_t\}$.

Now assume that $f(x)$ has r_1 roots in $\{\alpha_1,\alpha_2,\ldots,\alpha_t\}$ and r_2 roots in $\{\beta_1,\beta_2,\ldots,\beta_b\}$, then we have $r_1\leqslant\min\{3(m-1),t\}$ and $r_1+3r_2\leqslant deg\, f(x)\leqslant (q^2+q+1)(m-1)$.

Thus,

$$r_1+r_2=\frac{1}{3}(r_1+3r_2+2r_1)\leqslant\frac{1}{3}((q^2+q+1)(m-1)+2\cdot\min\{3(m-1),t\})$$

and

$$wt(\phi(f(x))=n-(r_1+r_2)\geqslant n-\frac{1}{3}((q^2+q+1)(m-1)+2\cdot\min\{3(m-1),t\}). \qquad \square$$

Remark 1. For the case $3|q$, i.e., characteristic of $\mathbb{F}_q$ is 3, we modify the definition of $e_{i,j,k}(x)$ as follows:

$$e_{i,j,k}=\begin{cases} x^{q^2i+qj+k} & \text{if } i=j=k, \\ x^{q^2i+qj+k}+x^{q^2j+qk+i}+x^{q^2k+qi+j} & \text{otherwise.}\end{cases}$$

Defining the code $C_3(t,b,m)$ in the same way and by arguments similar to the case $3\nmid q$, one can show that we get a code with the same length and dimension and with the minimum distance bound

$$d\geqslant n-\frac{1}{3}((q^2+q+1)(m-1)+\max\{3t-q,2\cdot\min\{m-1,t\}\}).$$

3. Extensions of arbitrary prime degrees

In this section we will generalize the construction in the previous section to an extension of an arbitrary prime degree p. We first introduce some notation to simplify the writing.

Consider the extension $\mathbb{F}_{q^p}/\mathbb{F}_q$ where p is a prime. There are no intermediate extensions (strictly) between $\mathbb{F}_q$ and $\mathbb{F}_{q^p}$ and every element β of $\mathbb{F}_{q^p}$ which is not in $\mathbb{F}_q$ belongs to a conjugacy class of size p: $\{\beta,\beta^q,\ldots,\beta^{q^{p-1}}\}$. There are exactly $\frac{q^p-q}{p}$ such conjugacy classes.

Let the vector $\boldsymbol{i}_p$ denote the p-tuple $(i_1,i_2,\ldots,i_p)$ of integers with $0\leqslant i_1\leqslant i_2\leqslant\cdots\leqslant i_p\leqslant m-1\leqslant q-1$. Let μ denote the left-cyclic-shift operation: $\mu(i_1,i_2,\ldots,i_p)=(i_2,i_3,\ldots,i_p,i_1)$ and let μ^n denote the n-fold composition of μ, cyclic shift by n positions. Let

$$e_{\boldsymbol{i}_p}(x)=\sum_{j=1}^{p}x^{(q^{p-1},q^{p-2},\ldots,1)\cdot\mu^j(i_1,i_2,\ldots,i_p)},$$

where $\cdot$ denotes the usual dot product. Again, one can show that $e_{\boldsymbol{i}_p}(\beta)^q=e_{\boldsymbol{i}_p}(\beta)$ and conclude that $e_{\boldsymbol{i}_p}(\beta)\in\mathbb{F}_q$ for any $\beta\in\mathbb{F}_{q^p}$. Let $V_{m,p}$ denote the $\mathbb{F}_q$-span of all polynomials $e_{\boldsymbol{i}_p}(x)$ with $0\leqslant i_1\leqslant i_2\leqslant\cdots\leqslant i_p\leqslant m-1\leqslant q-1$. Then for any $f(x)\in V_{m,p}$, $f(\beta)\in\mathbb{F}_q$ and $\dim V_{m,p}$ is $\frac{[m]^p}{p!}=\binom{m+p-1}{p}=\binom{m+p-1}{m-1}$ by Proposition 1. This dimension is the same as the dimension of the space $V_{s,m}$ introduced in [3, Lemma 2.4].

For $1\leqslant b\leqslant r=\frac{q^p-q}{p}$ and $1\leqslant m<1+\frac{bp(q-1)}{q^p-1}$ we define a code $C_p(b,m)$ over $\mathbb{F}_q$ as follows:

$$C_p(b,m)=\{(f(\beta_1),f(\beta_2),\ldots,f(\beta_b)):f\in V_{m,p}\},$$

where each β_i is from a distinct conjugacy class in $\mathbb{F}_{q^p}-\mathbb{F}_q$. Since we do not employ elements of $\mathbb{F}_q$ in this construction, the condition $(p,q)=1$ is not necessary. This is obviously a linear code of length $n=b\leqslant\frac{q^p-q}{p}$ over $\mathbb{F}_q$.

Proposition 4. *For $1\leqslant m<1+\frac{bp(q-1)}{q^p-1}$, the dimension of $C_p(b,m)$ is equal to $\frac{[m]^p}{p!}$.*

Proof. Similarly to Proposition 2, one verifies that the linear map

$$\phi : V_{m,p} \to \mathbb{F}_q^b,$$
$$f \to (f(\beta_1), f(\beta_2), \ldots, f(\beta_b))$$

is one to one. □

Proposition 5. *The minimum distance d of $C_p(b,m)$ satisfies*

$$d \geqslant b - \frac{m-1}{p} \cdot \frac{(q^p-1)}{q-1}.$$

Proof. Let $f(x) \in V_{m,p}$. Suppose $f(x)$ has r roots in $\{\beta_1, \beta_2, \ldots, \beta_b\}$, then $f(x)$ has at least pr roots. Therefore, $pr \leqslant deg\, f(x) \leqslant \frac{q^p-1}{q-1}(m-1)$ and $r \leqslant \frac{m-1}{p}\frac{q^p-1}{q-1}$. The weight of $\phi(f(x))$ is then $\geqslant b - r \geqslant b - \frac{m-1}{p}\frac{q^p-1}{q-1}$. □

Remark 2. As in Section 4.2, we could have used elements from $\mathbb{F}_q$ and defined

$$C_p(b,m) = \{(f(\alpha_1), \ldots, f(\alpha_t), f(\beta_1), \ldots, f(\beta_b)) : f \in V_{m,p}\}$$

for any $1 \leqslant t \leqslant q$ and carried out the analysis for the dimension and the minimum distance similarly.

3.1. Examples

Now we present examples of some optimal codes found by this construction. In all of these examples, $p = 3$, $m = 2$ so that the dimension is 4.

1. Let $q = 3$, $b = (3^3 - 3)/3 = 8$ and we get an $[8,4,4]_3$-code which is optimal by the Griesmer bound. By taking $b = 7$ and 6 we also find $[7,4,3]_3$ and $[6,4,2]_3$ codes, respectively, which are also optimal by the table [1].
2. Choosing $q = 4$, and $b = (4^3 - 4)/3 = 20$, a $[20,4,13]_4$-code is found. By checking the table [1], this code is also optimal. Choosing $b = 19$ and keeping the rest of the parameters the same, we find another optimal code; a $[19,4,12]_4$-code.
3. Taking $q = 5$ and $b = (5^3 - 5)/3 = 40$, one obtains a code with parameters $[40,4,30]_5$ which is optimal by the Griesmer bound.

3.2. An optimal family of three-dimensional codes

Taking $p = 2$, $m = 2$, and $b = \frac{q^2-q}{2} - a$ with $0 \leqslant a < \frac{q-1}{2}$ for odd q and $a < q$ for even q, one obtains codes with parameters $[n,k,d]_q$ over any field $\mathbb{F}_q$ with $q \geqslant 3$, where $n = b, k = 3$, and $d \geqslant n - \frac{q+1}{2} = \frac{q^2-2q-2a-1}{2}$. It turns out that these give *optimal* parameters.

Proposition 6. *Let a be as described, then a* $[\frac{q^2-q-2a}{2}, 3, d \geqslant \frac{q^2-2q-2a-1}{2}]_q$*-code is optimal over any field* $\mathbb{F}_q$.

Proof. We show that with these parameters the equality is attained in the Griesmer bound. It suffices to show that

$$n \leqslant \sum_{k=0}^{2} \left\lceil \frac{d}{q^k} \right\rceil = d + \left\lceil \frac{d}{q} \right\rceil + 1. \tag{1}$$

Case 1: q is odd. Inequality (1) is equivalent to

$$\frac{q-1}{2} \leqslant \left\lceil \frac{q^2 - 2q - 2a - 1}{2q} \right\rceil.$$

Since $\frac{q^2-2q-2a-1}{2q} > \frac{q-1}{2} - 1 = \frac{q-3}{2}$ for any q when $a < \frac{q-1}{2}$, the last inequality holds.

Case 2: q is even. We note that the minimum distance can be improved to $d \geqslant \frac{q^2-2q-2a}{2}$ in this case and we verify that the inequality in (1) is satisfied for $a < q$. □

4. Another class of polynomial codes

We assume the notation of the previous sections and let p denote an arbitrary (but fixed) prime throughout this section. Let K be a positive integer and let P_K denote the set of all polynomials of degree strictly less than K over $\mathbb{F}_q$. Then P_K is a K-dimensional vector space over $\mathbb{F}_q$. Next, for an integer b such that $b \leqslant \frac{q^p-q}{p}$ we define

$$V_{K,b} = \{f \in P_K : f(\beta_1), f(\beta_2), \ldots, f(\beta_b) \in \mathbb{F}_q\},$$

where as before each β_i is from a distinct conjugacy class of size p in $\mathbb{F}_{q^p} - \mathbb{F}_q$. It is easy to see that $V_{K,b}$ is a vector space (a subspace of P_K) over $\mathbb{F}_q$. We are interested in the dimension of it. The proof of the next lemma giving the dimension of this space for a special case uses The Chinese Remainder Theorem [2].

Lemma 1. *For* $K \geqslant bp$*, the dimension of* $V_{K,b}$ *is* $K - bp + b$.

Proof. Let $m_i(x)$ denote the minimal polynomial of β_i over $\mathbb{F}_q$ and let $M_j(x) = \prod_{i=1}^{j} m_i(x)$. The degrees of all of $m_i(x)$'s are equal to p, hence *deg* $M_b(x) = pb$.

Note that an element $f(x)$ of P_K is in $V_{K,b}$ if and only if $f(\beta_1) = \alpha_1$, $f(\beta_2) = \alpha_2, \ldots, f(\beta_b) = \alpha_b$ for some $(\alpha_1, \alpha_2, \ldots, \alpha_b) \in \mathbb{F}_q^b$. This holds if and only if $f(\beta_1) - \alpha_1 = 0, f(\beta_2) - \alpha_2 = 0, \ldots, f(\beta_b) - \alpha_b = 0$, or equivalently we have the

following divisibility relations:

$$m_1(x)|f(x)-\alpha_1, m_2(x)|f(x)-\alpha_2, \ldots, m_b(x)|f(x)-\alpha_b.$$

This means that $f(x)$ is a simultaneous solution to the set of congruences

$$\begin{cases} f(x) \equiv \alpha_1 \bmod m_1(x), \\ f(x) \equiv \alpha_2 \bmod m_2(x), \\ \qquad \vdots \\ f(x) \equiv \alpha_b \bmod m_b(x). \end{cases} \tag{2}$$

Since the polynomials $m_i(x)$, $1 \leqslant i \leqslant b$, are mutually coprime, there is a solution to the above system which is unique mod $M_b(x)$ by the Chinese Remainder Theorem. To find the dimension of $V_{K,b}$, we count the number of solutions of (2) which are in $V_{K,b}$. For every $(\alpha_1, \alpha_2, \ldots, \alpha_b) \in \mathbb{F}_q^b$, there is a unique $f(x) \in \mathbb{F}_q[x]/\langle M_b(x) \rangle$ satisfying (2) and all the solutions in $\mathbb{F}_q[x]$ are of the form $F(x) = f(x) + M_b(x)t(x)$ for some $t(x) \in \mathbb{F}_q[x]$. A solution $F(x)$ is in $V_{K,b}$ if and only if $deg\, t(x) < K - pb$ and there are q^{K-bp} such polynomials. Therefore, the total number of solutions is q^{K-bp+b} if $K \geqslant pb$, and the dimension of $V_{K,b}$ is $K - bp + b$. □

For $K = pb$, let us denote $V_{K,b}$ by V_b whose dimension is b. V_b has a basis consisting of b elements $E_b = \{e_1, e_2, \ldots, e_b\}$. We can assume that the degrees of the basis elements are distinct, because we can take each e_i to be monic and if two elements e_m, e_n have the same degree then we can replace them by $e_m, e_m - e_n$. So we also assume $deg\, e_1 < deg\, e_2 < \cdots < deg\, e_b$. For a positive integer r with $r < \frac{b}{p}$, consider the subspace $V_{b,r}$ generated by $E_b - \{e_{b-rp+1}, e_{b-rp+2}, \ldots, e_b\} = \{e_1, e_2, \ldots, e_{b-rp}\}$. Note that the degree of an element in $V_{b,r}$ is strictly less than $pb - rp$. Now we use the space $V_{b,r}$ to construct a class of polynomial codes.

Theorem 1. *For any prime p, $b \leqslant \frac{q^p - q}{p}$, and $r < \frac{b}{p}$ there exists a linear code with parameters $[b, b - rp, r + 1]$ over $\mathbb{F}_q$.*

Proof. Let

$$C(m, r, b) = \{(f(\beta_1), f(\beta_2), \ldots, f(\beta_b)),\ f \in V_{b,r}\}.$$

Then it is obvious that $C(m, r, b)$ is a linear code of length b and dimension $b - rp$. It is also not difficult to see that the minimum weight is $\geqslant r + 1$ from the degree restriction. So we get a family of codes with parameters $[b, b - rp, r + 1]$ over $\mathbb{F}_q$. □

By choosing the parameters suitably, we show that some *near-optimal* codes can be obtained by this construction. By a near-optimal code we mean a code whose minimum distance is at most one less than that of a d-optimal code.

Example 1. Letting $p=3, b=\frac{q^3-q}{3}$ and $r=2$, we obtain a family of codes with parameters $[b, b-6, 3]$ over any finite field $\mathbb{F}_q$. The sphere packing bound shows that the minimum distance of a linear code with this length and dimension is at most 4 if $q \geqslant 5$. Therefore, this family of codes are near-optimal for $q \geqslant 5$.

If we choose $p=2, b=\frac{q^2-q}{2}$, and $r=4$, we obtain a code with parameters $[b, b-8, 5]$ over $\mathbb{F}_q$. Again by the sphere packing bound, the minimum distance of a linear code with this length and dimension cannot be $\geqslant 7$ if $q \geqslant 59$. Therefore, we obtain another family of near-optimal codes.

If $p=5, b=\frac{q^5-q}{5}$, and $r=2$, we obtain a $[b, b-10, 3]_q$-code. Again, one checks that the minimum distance of this code cannot be larger than 4 for $q \geqslant 9$ by the sphere packing bound.

4.1. The case $K<bp$

For $K \geqslant bp$ we have shown that the dimension of the space $V_{K,b}$ is $K-bp+b$. For our purposes, the complementary case $K<bp$ is more interesting. To investigate the dimension in that case, we note that for a polynomial $f(x)=\sum_{i=0}^{K-1} a_i x^i$ in $\mathbb{F}_q[x]$, $f(\beta) \in \mathbb{F}_q$ if and only if $f^q(\beta)=f(\beta)$ which is equivalent to

$$\sum_{i=0}^{K-1} a_i(\beta^{iq}-\beta^i)=0.$$

Therefore, $f(\beta_j) \in \mathbb{F}_q$, $1 \leqslant j \leqslant b$ means $\sum_{i=0}^{K-1} a_i(\beta_j^{iq}-\beta_j^i)=0$, $1 \leqslant j \leqslant b$. Equivalently, $f(x) \in V_{K,b}$ if and only if $(a_1, a_2, \ldots, a_{K-1})$ is in the null space of the $b \times (K-1)$ matrix

$$M=\begin{bmatrix} \beta_1^q-\beta_1 & \beta_1^{2q}-\beta_1^2 & \ldots & \beta_1^{(K-1)q}-\beta_1^{K-1} \\ \beta_2^q-\beta_2 & \beta_2^{2q}-\beta_2^2 & \ldots & \beta_2^{(K-1)q}-\beta_2^{K-1} \\ \vdots & & & \vdots \\ \beta_b^q-\beta_b & \beta_b^{2q}-\beta_b^2 & \ldots & \beta_b^{(K-1)q}-\beta_b^{K-1} \end{bmatrix}.$$

Hence, the dimension of $V_{K,b}$ is equal to the nullity of M over $\mathbb{F}_q$ plus 1. The matrix M can be written as a $bp \times (K-1)$ matrix M_q over $\mathbb{F}_q$ by replacing every entry as a column vector of length p over $\mathbb{F}_q$. In particular, the nullity of M_q is equal to $b-1$ when $K=bp$.

4.2. Examples

We compute the nullity of M_q for various values of the parameters and obtain a number of codes that have the same parameters as the presently best-known codes.

In particular, for $q = 5, p = 3, b = 40$ and $K = 93$, we find a code with length 40, dimension 23 and minimum distance $\geqslant 10$ over $\mathbb{F}_5$. According to [1], this is a new linear code. We used the Computer Algebra system Maple to carry out the computations in finite fields. Below are some of the parameters of the codes we obtain by this construction.

Parameters of codes obtained by the method described in Section 4.1

q	p	b	K	**Parameters**	**Comments**
3	3	8	21	[8,6,2]	Optimal
3	5	48	230	[48,42,3]	Optimal
5	3	40	117	[40,38,2]	Optimal
5	3	40	114	[40,36,3]	Optimal
5	3	40	96	[40,24,9]	Best-known
5	3	40	93	[40,23,10]	New
5	3	40	90	[40,20,11]	Best-known
5	3	40	87	[40,19,12]	Best-known
5	3	40	84	[40,17,13]	Best-known
5	3	40	81	[40,15,14]	Best-known
5	3	40	78	[40,14,15]	Best-known
5	3	39	92	[39,23,9]	Best-known
5	3	38	92	[38,23,8]	Best-known
7	2	21	38	[21,18,3]	Optimal
7	2	21	36	[21,16,4]	Best-known
7	2	21	34	[21,15,5]	Best-known
7	2	21	32	[21,14,6]	Best-known
7	2	21	30	[21,12,7]	Best-known
7	2	21	26	[21,10,9]	Best-known
7	2	21	24	[21,9,10]	Best-known
7	2	20	34	[20,15,4]	Best-known
7	2	20	32	[20,14,5]	Best-known
7	2	20	30	[20,12,6]	Best-known
7	2	19	32	[19,14,4]	Best-known
7	2	19	34	[19,16,13]	Optimal

Acknowledgments

The authors thank the anonymous reviewers for their useful comments, suggestions and corrections which improved the paper.

References

[1] A.E. Brouwer, Linear code bound (on-line server), Eindhoven University of Technology, The Netherlands, http://www.win.tue.nl/~aeb/voorlincod.html.
[2] D.S. Dummit, R.M. Foote, Abstract Algebra, Princeton-Hall, Englewood Cliffs, NJ, 1991.
[3] S. Ling, H. Niederreiter, C. Xing, Symmetric polynomials and some good codes, Finite Fields Appl. 7 (2001) 142–148.
[4] C. Xing, S. Ling, A class of linear codes with good parameters, IEEE Trans. Inform. Theory 46 (2000) 2184–2188.